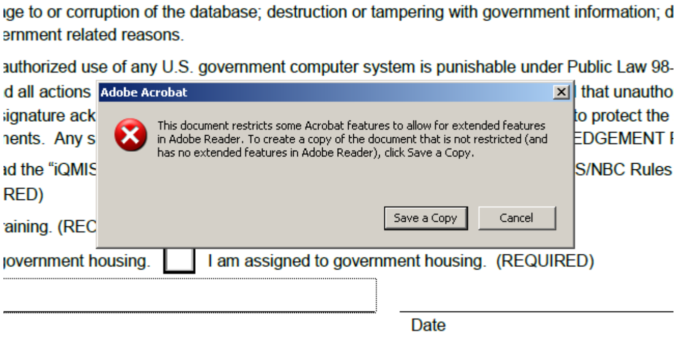
Digital Signatures on iQMIS User Access Request Form

When a user clicks in the “User Signature block” on the iQMIS Access Form, the following window appears:



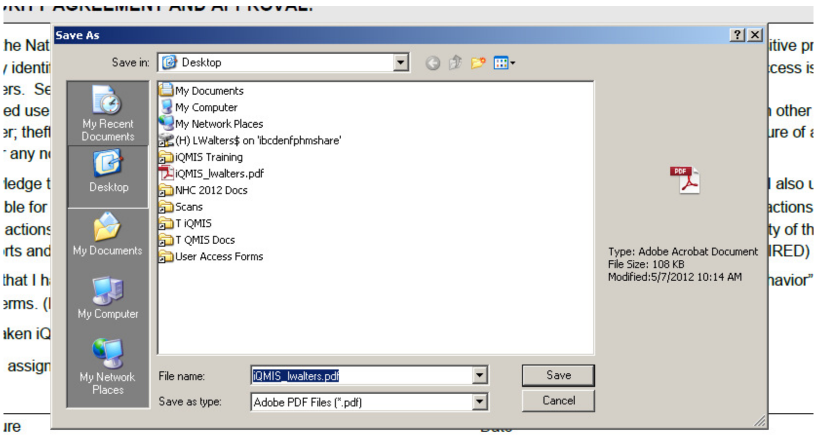
Adobe Acrobat

This document restricts some Acrobat features to allow for extended features in Adobe Reader. To create a copy of the document that is not restricted (and has no extended features in Adobe Reader), click Save a Copy.

Click “Save a Copy” and rename it with your name, such as “iQMIS_JJones” or “iQMIS_KChapman.” This is a copy of the completed form, but it is not signed yet.

Open this copy and click in the User’s Signature Block. Information will display regarding your Digital ID.

Then the following window appears:



Save As

Save in: Desktop

File name: iQMIS_lwalters.pdf

Save as type: Adobe PDF Files (*.pdf)

Type: Adobe Acrobat Document
File Size: 108 KB
Modified:5/7/2012 10:14 AM

You must save a second copy of the form in order to sign it and save it as a signed document. Create a new name, such as “Signed_iQMIS_JJones” or “Signed_iQMIS_KChapman,” and click “Save.” If you use your Smart Card – the HPSD 12 Federal ID Card – it will ask for your ID card’s PIN. This is not the password for your Digital ID.

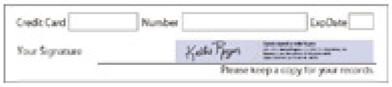
You can then save the signed document and email it to your approver (see “Instructions” for your Agency’s specific approver,) or deliver the printed document to your approver.

About Digital Signatures
From
http://help.adobe.com/en_US/acrobat/standard/using/WS58a04a822e3e50102bd615109794195ff-7d4a.w.html

A *digital signature*, like a conventional handwritten signature, identifies the person signing a document. Unlike a handwritten signature, a digital signature is difficult to forge because it contains encrypted information that is unique to the signer. It can be easily verified and informs recipients whether the document was modified after the signer initially signed the document.

To sign a document, you must obtain a digital ID or create a self-signed digital ID in Acrobat or Adobe Reader. The digital ID contains a private key and a certificate with a public key and more. The private key is used to create the digital signature. The certificate is a credential that is automatically applied to the signed document. The signature is verified when recipients open the document.

When you apply a digital signature, Acrobat uses a hashing algorithm to generate a message digest, which it encrypts using your private key. Acrobat embeds the encrypted message digest in the PDF, certificate details, signature image, and a version of the document when it was signed.



Credit Card Number ExpDate
Your Signature
Please keep a copy for your records.

Digital signature in a PDF form

What is a digital ID?

From http://help.adobe.com/en_US/acrobat/standard/using/WS11dd809af63f0e1e-43e0464b12b4384d3b6-8000.html

Digital IDs include a private key that you safeguard and a public key (certificate) that you share. A *digital ID* is like an electronic driver's license or passport that proves your identity. A digital ID usually contains your name and email address, the name of the organization that issued it, a serial number, and an expiration date. Digital IDs are used for certificate security and digital signatures.

Digital IDs contain two keys: the *public key* locks, or encrypts data; the *private key* unlocks, or decrypts that data. When you sign PDFs, you use the private key to apply your digital signature. The public key is in a *certificate* that you distribute to others. For example, you can send the certificate to those who want to validate your signature or identity. Store your digital ID in a safe place, because it contains your private key that others can use to decrypt your information.

Why do I need one?
You don't need a digital ID for most of the work you do in PDFs. For example, you don't need a digital ID to create PDFs, comment on them, and edit them. You need a digital ID to sign a document or encrypt PDFs through a certificate.

How do I get one?
You can get a digital ID from a third-party provider, or you can create a self-signed digital ID.

Self-signed digital IDs

Self-signed digital IDs can be adequate for personal use or small-to-medium businesses. Their use should be limited to parties that have established mutual trust.

IDs from certificate authorities

Most business transactions require a digital ID from a trusted third-party provider, called a *certificate authority*. Because the certificate authority is responsible for verifying your identity to others, choose one that is trusted by major companies doing business on the Internet. The Adobe website gives the names of Adobe security partners that offer digital IDs and other security solutions. See Adobe Security Partner Community at www.adobe.com/security/partners/index.html.

Create a self-signed digital ID

Sensitive transactions between businesses generally require an ID from a certificate authority rather than a self-signed one.

1. Do one of the following:
    - In Acrobat, choose Tools > Sign & Certify > More Sign & Certify > Security Settings.
    - In Reader, choose Edit > Protection > Security Settings.

Note: If you don't see the Sign & Certify or Protection panel, see the instructions for adding panels at Task panes.

2. Select Digital IDs on the left, and then click the Add ID button .
3. Select the option A New Digital ID I Want To Create Now, and click Next.
4. Specify where to store the digital ID, and click Next.
    - New PKCS#12 Digital ID File -- Stores the digital ID information in a file, which has the extension .pfx in Windows and .p12 in Mac OS. You can use the files interchangeably between operating systems. If you move a file from one operating system to another, Acrobat still recognizes it.
    - Windows Certificate Store (Windows only) -- Stores the digital ID to a common location from where other Windows applications can also retrieve it.
5. Type a name, email address, and other personal information for your digital ID. When you certify or sign a document, the name appears in the Signatures panel and in the Signature field.
6. (Optional) To use Unicode values for extended characters, select Enable Unicode Support, and then specify Unicode values in the appropriate boxes.
7. Choose an option from the Key Algorithm menu. The 2048-bit RSA option offers more security than 1024-bit RSA, but 1024-bit RSA is more universally compatible.
8. From the Use Digital ID For menu, choose whether you want to use the digital ID for signatures, data encryption, or both.
9. Type a password for the digital ID file. For each keystroke, the password strength meter evaluates your password and indicates the password strength using color patterns. Reconfirm your password.

    You can export and send your certificate file to contacts who can use it to validate your signature.

Important: Make a backup copy of your digital ID file. If your digital ID file is lost or corrupted, or if you forget your password, you cannot use that profile to add signatures.

Register a digital ID

To use your digital ID, register your ID with Acrobat or Reader.

1. Do one of the following:
    - In Acrobat, choose Tools > Protection > More Protection > Security Settings.
    - In Reader, choose Edit > Protection > Security Settings.

    Note: If you don't see the Protection panel, see the instructions for adding panels at Task panes.
2. Select Digital IDs on the left.
3. Click the Add ID button .
4. Select My Existing Digital ID From and choose one of the following options:
    - A File -- Select this option if you obtained a digital ID as an electronic file. Follow the prompts to select the digital ID file, type your password, and add the digital ID to the list.
    - A Roaming Digital ID Stored On A Server -- Select this option to use a digital ID that's stored on a signing server. When prompted, type the server name and URL where the roaming ID is located.
    - A Device Connected To This Computer

    Select this option if you have a security token or hardware token connected to your computer.
5. Click Next, and follow the onscreen instructions to register your digital ID.

Specify the default digital ID

To avoid being prompted to select a digital ID each time your sign or certify a PDF, you can select a default digital ID.

1. Do one of the following:
    - In Acrobat, choose Tools > Protection > More Protection > Security Settings.
    - In Reader, choose Edit > Protection > Security Settings.

    Note: If you don't see the Protection panel, see the instructions for adding panels at Task panes.
2. Click Digital IDs on the left, and then select the digital ID you want to use as the default.
3. Click the Usage Options button ✏, and choose a task for which you want the digital ID as the default. To specify the digital ID as the default for two tasks, click the Usage Options button again and select a second option.

A check mark appears next to selected options. If you select only the signing option, the Sign icon 🖊 appears next to the digital ID. If you select only the encryption option, the Lock icon 🔒 appears. If you select only the certifying option, or if you select the signing and certifying options, the Blue Ribbon icon 🎗 appears.

💡 To clear a default digital ID, repeat these steps, and deselect the usage options you selected.

Change the password and timeout for a digital ID

Passwords and timeouts can be set for PKCS #12 IDs. If the PKCS #12 ID contains multiple IDs, configure the password and timeout at the file level.

Note: Self-signed digital IDs expire in five years. After the expiration date, you can use the ID to open, but not sign or encrypt, a document.

1. Do one of the following:

- In Acrobat, choose Tools > Protection > More Protection > Security Settings.
- In Reader, choose Edit > Protection > Security Settings.

Note: If you don’t see the Protection panel, see the instructions for adding panels at Task panes.

2. Expand Digital IDs on the left, select Digital ID Files, and then select a digital ID on the right.
3. Click the Change Password button. Type the old password and a new password. For each keystroke, the password strength meter evaluates your password and indicates the password strength using color patterns. Confirm the new password, and then click OK.
4. With the ID still selected, click the Password Timeout button.
5. Specify how often you want to be prompted for a password:
    - Always -- Prompts you each time you use the digital ID.
    - After -- Lets you specify an interval.
    - Once Per Session -- Prompts you once each time you open Acrobat.
    - Never -- You’re never prompted for a password.
6. Type the password, and click OK.

💡 Be sure to back up your password in a secure place. If you lose your password, either create a new self-signed digital ID and delete the old one, or purchase one from a third-party provider.

Delete your digital ID

When you delete a digital ID in Acrobat, you delete the actual PKCS #12 file that contains both the private key and the certificate. Before you delete your digital ID, ensure that it isn’t in use by other programs or required by any documents for decrypting.

Note: You can delete only self-signed digital IDs that you created in Acrobat. A digital ID obtained from another provider cannot be deleted.

1. Do one of the following:
    - In Acrobat, choose Tools > Protection > More Protection > Security Settings.
    - In Reader, choose Edit > Protection > Security Settings.

Note: If you don’t see the Protection panel, see the instructions for adding panels at Task panes.

2. Select Digital IDs on the left, and then select the digital ID to remove.
3. Click Remove ID, and then click OK.

Protecting digital IDs

By protecting your digital IDs, you can prevent unauthorized use of your private keys for signing or decrypting confidential documents. Ensure that you have a procedure in place in the event your digital ID is lost or stolen.

How to protect your digital IDs

When private keys are stored on hardware tokens, smart cards, and other hardware devices that are password- or PIN-protected, use a strong password or PIN. Never divulge your password to others. If you must write down your password, store it in a secure location. Contact your system administrator for guidelines on choosing a strong password. Keep your password strong by following these rules:

- Use eight or more characters.
- Mix uppercase and lowercase letters with numbers and special characters.
- Choose a password that is difficult to guess or hack, but that you can remember without having to write it down.

- Do not use a correctly spelled word in any language, as they are subject to “dictionary attacks” that can crack these passwords in minutes.
- Change your password on a regular basis.
- Contact your system administrator for guidelines on choosing a strong password.

To protect private keys stored in P12/PFX files, use a strong password and set your password timeout options appropriately. If using a P12 file to store private keys that you use for signing, use the default setting for password timeout option. This setting ensures that your password is always required. If using your P12 file to store private keys that are used to decrypt documents, make a backup copy of your private key or P12 file. You can use the backed up private key of P12 file to open encrypted documents if you lose your keys.

The mechanisms used to protect private keys stored in the Windows certificate store vary depending on the company that has provided the storage. Contact the provider to determine how to back up and protect these keys from unauthorized access. In general, use the strongest authentication mechanism available and create a strong password or PIN when possible.

What to do if a digital ID is lost or stolen

If your digital ID was issued by a certificate authority, immediately notify the certificate authority and request the revocation of your certificate. In addition, you should not use your private key.

If your digital ID was self-issued, destroy the private key and notify anyone to whom you sent the corresponding public key (certificate).

Smart cards and hardware tokens

A *smart card* looks like a credit card and stores your digital ID on an embedded microprocessor chip. Use the digital ID on a smart card to sign and decrypt documents on computers that can be connected to a smart card reader. Some smart card readers include a keypad for typing a personal identification number (PIN).

Similarly, a *security hardware token* is a small, keychain-sized device that you can use to store digital IDs and authentication data. You can access your digital ID by connecting the token to a USB port on your computer or mobile device.

If you store your digital ID on a smart card or hardware token, connect it to your device to use it for signing documents.